



20192233 박진철  
7차 세미나 피드백 및 문제 개발

**FaS 8차 세미나**

목차

× +

kookmin univ.

⋮

+ New chat

☐

Today

☞ 폰 루팅

☞ 팀업 복호화

☞ 문제 초안

👤 FaS 세미나

20192233 박진철

CONTENTS

📱

폰 루팅

루팅이란

루팅 폰 정보

참고 사이트

루팅 과정

💬

TeamUP 복호화

진행상황

DB 복호화

DB 속 정보

📋

문제 초안

문제 초안 1

문제 초안 2

Send a message

➤

1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# 루팅이란

루팅: 최고 관리자 권한 root를 사용할 수 없는 시스템에서 root를 사용할 수 있게 하는 것

휴대폰 루팅으로 할 수 있는 것들

- 하드웨어 성능 조절
- 배터리 충전 제어
- 게임 해킹
- 애플리케이션 데이터 추출

⇒ 루팅을 통해 분석에 필요한 데이터 추출 가능

Send a message

1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

루팅 폰 정보

 휴대폰 기종: 구글 Pixel 4a(2020년 출시)



-OS: 안드로이드 13

-구글에 부트 이미지가 올라와 있음  
→루팅에 용이

Send a message

1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅


팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

참고 사이트



<https://youtu.be/XkxzA7av-iU>


<How to Root the Pixel 4a>

HOW TO

Root Android 11 on the Pixel 4a – Every Step Covered in Detail

BY DALLAS THOMAS 09/10/2020 8:43 AM 11/03/2020 7:13 AM TWEAKS & HACKS ROOT YOUR PHONE GOOGLE PIXEL TIPS, TRICKS & NEWS MAGISK 101

If you live in the US, it's pretty simple: The Google Pixel 4a is the [best phone for rooting and modding in 2020](#). Its price keeps the risk-reward ratio nice and low, and its unlockable bootloader makes it easy to modify virtually any aspect of Android.



But recent updates to Android's security systems have made it to where [TWRP](#) and other custom recoveries won't be officially available for this phone for quite some time, if at all. So you can't just install TeamWin and use it to flash a ZIP to root — you have to do things through Fastboot.

You'll be downloading a file from Google, using the Canary version of Magisk Manager to modify it since the regular version won't work with Android 11, then using your computer to flash it onto your Pixel 4a. But if that all sounds like Greek

<https://pixel.gadgethacks.com/how-to/root-android-11-pixel-4a-every-step-covered-detail-0333038/>

<Root Android 11 on the Pixel 4a>

Send a message

1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

루팅 과정 - 1. 개발자 옵션 활성화

휴대전화 정보

Android 버전  
13

기기 식별자

IP 주소  
fe80::d40f:53ff:fe8f:4a2e  
192.168.0.20

Wi-Fi MAC 주소  
확인하려면 저장된 네트워크를 선택하세요.

기기 Wi-Fi MAC 주소  
88:54:1f:4c:41:5d

블루투스 주소  
88:54:1f:4c:41:5c

가동 시간  
19:54:31

이 기기에 대한 의견 보내기

이미 개발자입니다.

빌드 번호  
TQ1A.221205.011

개발자 권한 부여

개발자 옵션

개발자 옵션 사용

USB 디버깅을 허용하시겠습니까?  
USB 디버깅은 개발용으로만 설계되었습니다. 이 기능을 사용하면 컴퓨터와 기기 간에 데이터를 복사하고 알림 없이 기기에 앱을 설치하며 로그 데이터를 읽을 수 있습니다.

취소 확인

USB가 연결된 경우 디버그 모드 사용

USB 디버깅 권한 승인 취소

무선 디버깅

adb 승인 시간 제한 사용 중지

USB 디버깅 허용

Send a message

1. 폰 루팅

+

← → ↺ kookmin univ.

+ New chat

☐

Today

☐ 폰 루팅

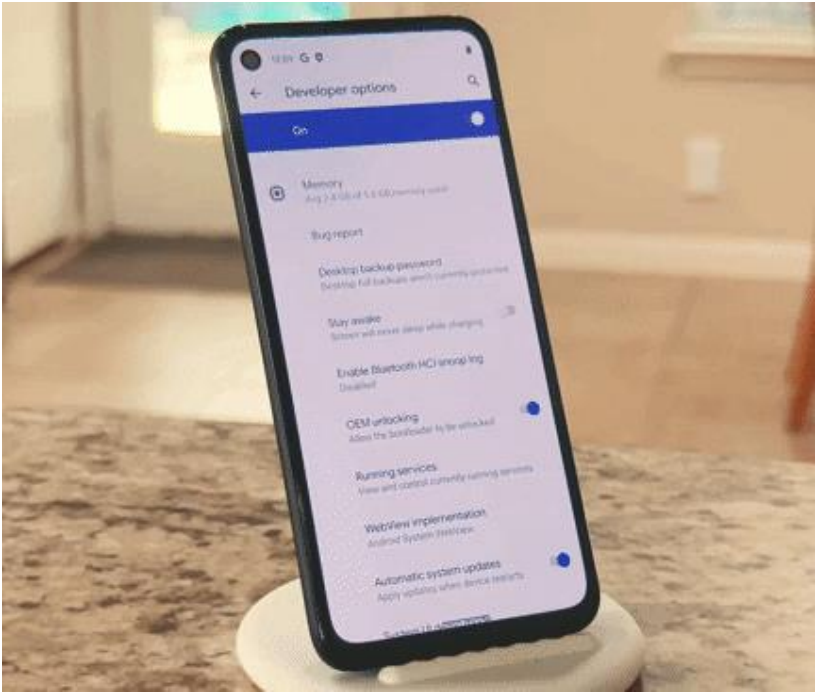

☐ 팀업 복호화

☐ 문제 초안

👤 FaS 세미나

20192233 박진철

# 루팅 과정 - 2. 부트로더 Unlock



## Google USB 드라이버 가져오기

Google 기기를 사용하는 Windows에서 adb 디버깅을 실행하려면 Google USB 드라이버가 필요합니다. 다른 모든 기기의 Windows 드라이버는 각 하드웨어 제조업체에서 제공하며 이 업체는 OEM USB 드라이버 설치에 나열되어 있습니다.

★ 참고: macOS 또는 Linux에서 개발하는 경우 USB 드라이버를 설치할 필요가 없습니다. 대신 하드웨어 기기에서 앱 실행을 참고하세요.

Windows용 Google USB 드라이버를 다운로드하는 방법에는 두 가지가 있습니다.

- Google USB 드라이버 ZIP 파일(ZIP) 다운로드
- 다음과 같이 Android SDK Manager에서 다운로드
  - Android 스튜디오에서 Tools > SDK Manager를 클릭합니다.
  - SDK Tools 탭을 클릭합니다.
  - Google USB Driver를 선택하고 OK를 클릭합니다.

FastBoot 모드 접속

Google USB 드라이버 설치

Send a message

➤

1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅


팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# 루팅 과정 - 2. 부트로더 Unlock



## SDK Platform Tools release notes

Android SDK Platform-Tools is a component for the Android SDK. It includes tools that interface with the Android platform, primarily `adb` and `fastboot`. Although `adb` is required for Android app development, app developers will normally just use the copy Studio installs. This download is useful if you want to use `adb` directly from the command-line and don't have Studio installed. (If you do have Studio installed, you might want to just use the copy it installed because Studio will automatically update it.) `fastboot` is needed if you want to unlock your device bootloader and flash it with a new system image. This package used to contain `sysrtrace`, but that has been obsoleted in favor of Studio Profiler, `gpuinspector.dev`, or `Perfetto`.

Although some new features in `adb` and `fastboot` are available only for recent versions of Android, they're backward compatible, so you should only need the latest version of the SDK Platform-Tools and should file bugs if you find exceptions.

### Downloads

If you're an Android developer, you should get the latest SDK Platform-Tools from Android Studio's [SDK Manager](#) or from the `sdkmanager` command-line tool. This ensures the tools are saved to the right place with the rest of your Android SDK tools and easily updated.

But if you want just these command-line tools, use the following links:

- [Download SDK Platform-Tools for Windows](#)

```
C:\Users\WJin_Cheol>
C:\Users\WJin_Cheol>cd C:\Users\WJin_Cheol\Documents\FaSW7발표\platform-tools
C:\Users\WJin_Cheol\Documents\FaSW7발표\platform-tools>fastboot flashing unlock_
```



부트로더 Unlock 완료

Send a message



1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

루팅 과정 - 3. 부트 이미지 다운

12:56

developers.google.com/andr

Google Play ser...

translated by Google

이 페이지는 Cloud Translation API를 통해 번역되었습니다.

Switch to English

홈 > 제품 > Google Play services > 다운로드

도움이 되었나요?

Nexus 및 Pixel 기기용 공장 출고 시 이미지

이 페이지의 내용

Pixel 6, Pixel 6 Pro, Pixel 6a 기기를 Android 13으로 처음 업데이트하는 경우

이용약관

Android Flash Tool 사용

플래시 지침

Pixel Tablet용 'tangorpro'

이 페이지에는 Nexus 또는 Pixel 기기의 공장 출고 시 펌웨어를 복원할 수 있는 바이너리 이미지 파일이 포함되어 있습니다. 이러한 파일은 기기에서 맞춤 빌드를 플래시한 후 기기를 출고 시 상태로 되돌리려는 경우에 유용합니다.

일반적으로 전체 OTA 이미지를 다운로드하는 것이

12:56

다운로드

전체 image-sunfish-tq1a.221205.011 sunfish-tq

1GB 초과

product.img 2.51GB, 23시간 전

100MB-1GB

system.img 867MB, 23시간 전

vendor.img 651MB, 23시간 전

system\_ext.img 314MB, 23시간 전

20-100MB

boot.img 67.11MB, 23시간 전

system\_other.img 25.83MB, 23시간 전

1-10MB

Send a message

1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

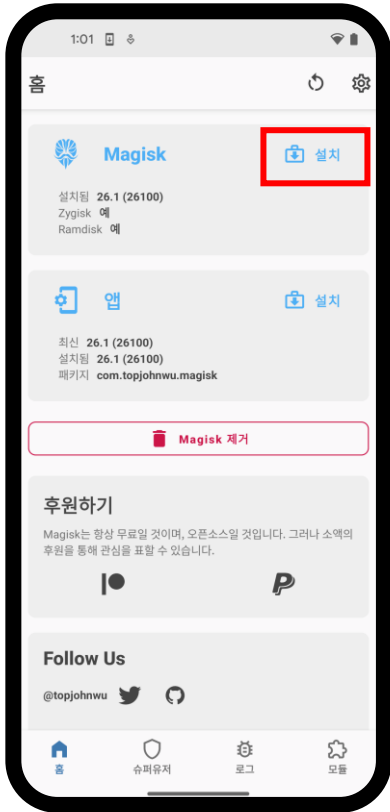
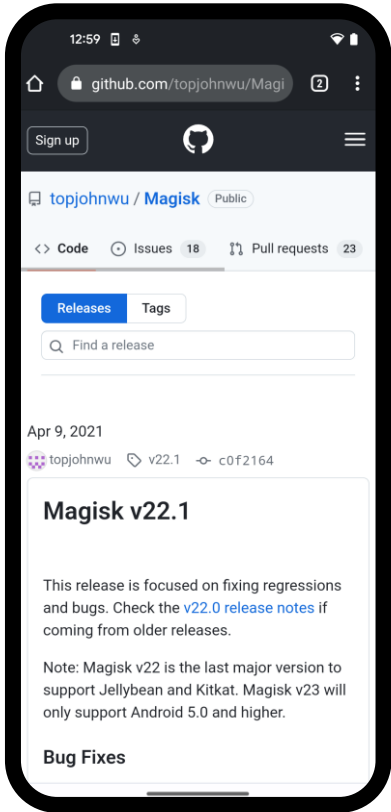

문제 초안

FaS 세미나

20192233 박진철

Send a message

# 루팅 과정 - 4. Magisk 다운



1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# 루팅 과정 - 5. 루팅 활성화



IMG



magisk\_patched-26100\_vm7ld.img

```
C:\Users\WJin_Cheol\Documents\FaSW7발표\platform-tools>fastboot flash boot C:\Users\WJin_Cheol\Documents\FaSW8발표\magisk_patched-26100_vm7ld.img_
```

Magisk에서 나온 이미지 파일을 이용하여 루트 권한 획득

Send a message

1. 폰 루팅

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# 루팅 과정 - 5. 루팅 활성화



Magisk에서 나온 이미지 파일을 이용하여 루트 권한 획득

Send a message

+ New chat

Today

폰 루팅

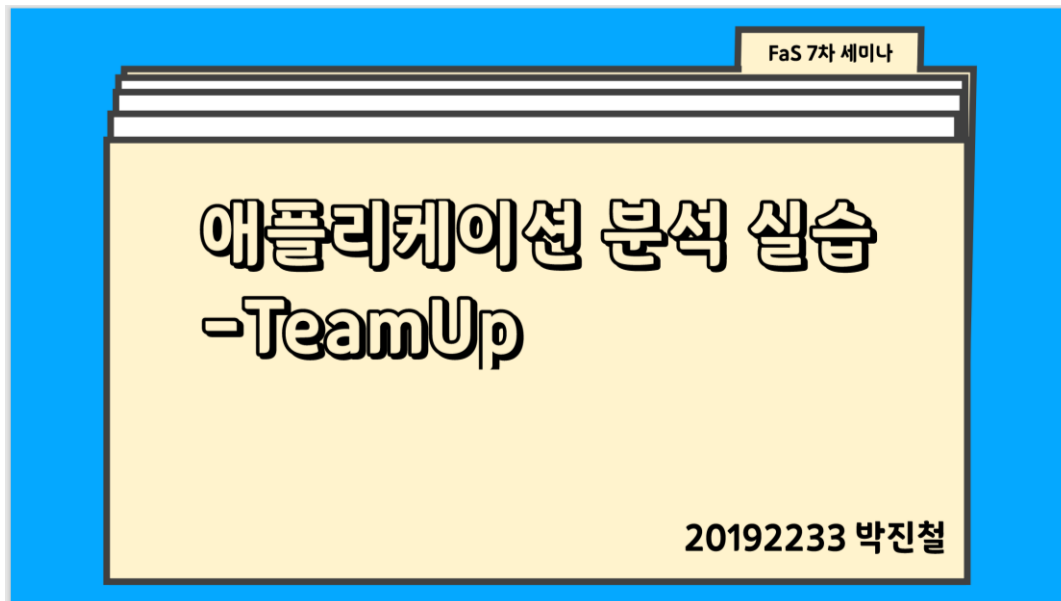
팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

## 7차 세미나까지 진행 상황



- TeamUP 아티팩트 적립
- 데이터 추출(녹스)
- 데이터베이스 복호화 코드 작성
- android\_id 획득 실패

⇒ 데이터는 추출하였으나 **android\_id**를 얻지 못함  
**루팅 폰**이 아닌 녹스를 이용하여 데이터를 추출

Send a message

+ New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# DB 복호화 - 1. 루팅 폰으로 파일 추출



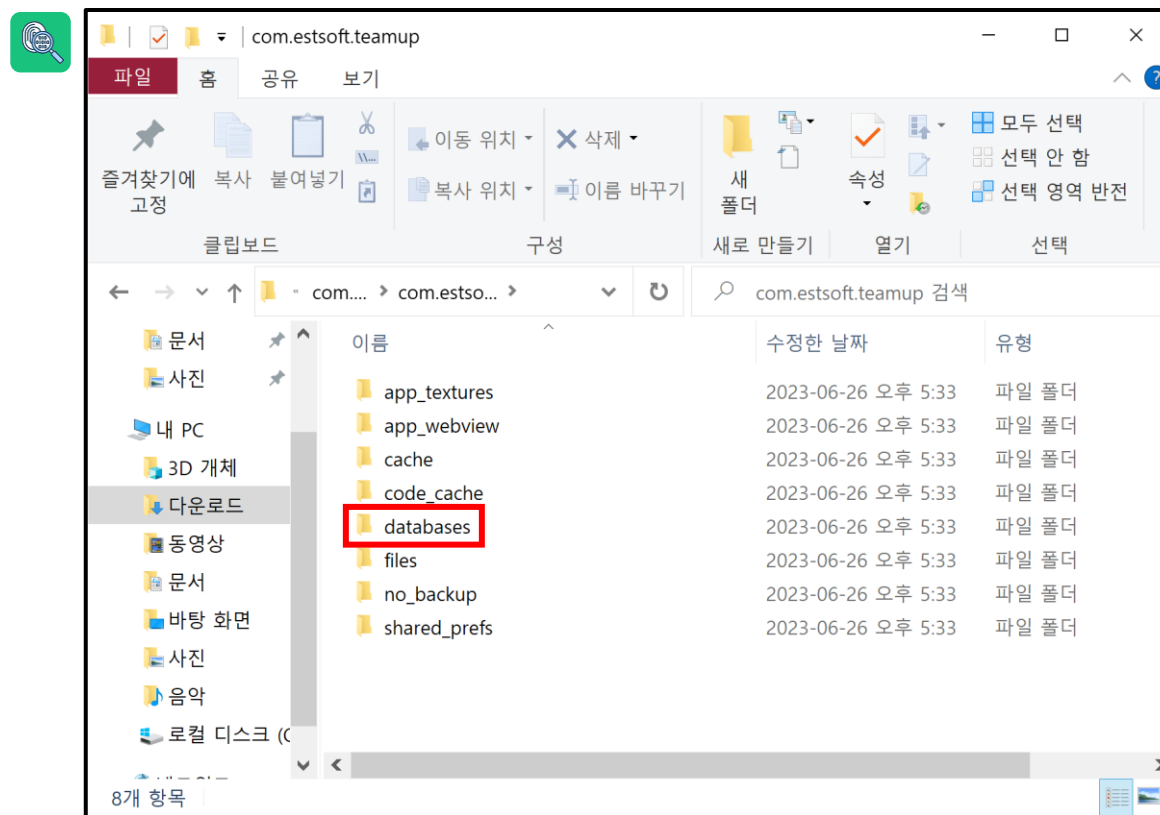
```
명령 프롬프트
C:\Users\Jin_Cheol>adb devices
List of devices attached
08111JEC212570 device

C:\Users\Jin_Cheol>adb shell
sunfish:/ $ su
sunfish:/ # cd /data/data/
sunfish:/data/data # ls
android
android.auto_generated_rro_product__
android.auto_generated_rro_vendor__
android.autoinstall.config.google.nexus
com.alphainventor.filemanager
com.android.backupconfirm
com.verizon.obdm
com.verizon.obdm_permissions
com.verizon.services
com.vzw.apnlib
deviceinfo.systeminfo.cpu.device.system
me.bridgefy.main
org.codeaurora.ims
vendor.qti.hardware.cacert.server
vendor.qti.iwlan
sunfish:/data/data # cp -r /data/data/com.estsoft.teamup /sdcard
sunfish:/data/data # exit
sunfish:/ $ exit
```

Adb shell로 TeamUP 데이터 획득

Send a message

# DB 복호화 - 1. 루팅 폰으로 파일 추출



- com.google.android.datatransport.events
- com.google.android.datatransport.event...
- google\_analytics\_v4.db
- google\_analytics\_v4.db-journal
- google\_app\_measurement\_local.db
- google\_app\_measurement\_local.db-jour...
- sending\_chat\_database
- sending\_chat\_database-shm
- sending\_chat\_database-wal
- TeamUP\_v5.db**

Adb shell로 TeamUP 데이터 획득

Send a message

+ New chat

Today

폰 루팅

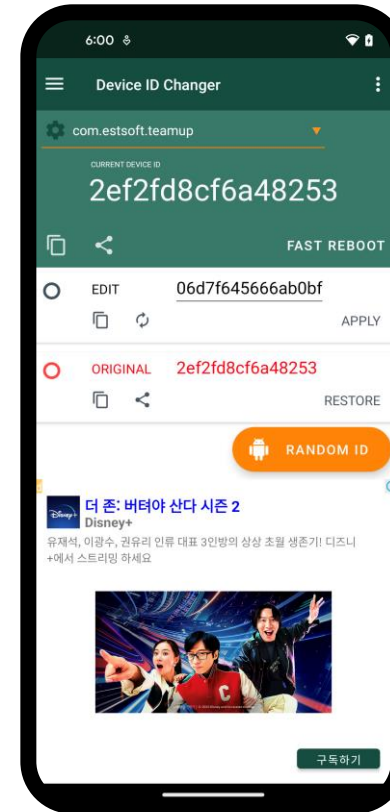
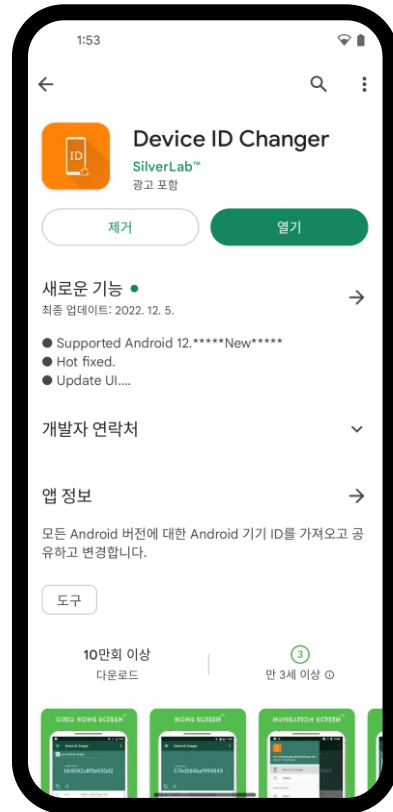
팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

## DB 복호화 - 2. android\_id 획득



Device ID Changer를 통해 android\_id 획득

Send a message



## DB 복호화 - 3. 키 획득 및 복호화



```
1 import hashlib as hash
2 import base64
3 from Crypto.Cipher import AES
4 from Crypto.Util.Padding import pad
5
6 and_id="2ef2fd8cf6a48253"
7
8 msg_digest=hash.sha256(and_id.encode()).digest()
9 str_Buffer=""
10 for b in msg_digest:
11     str_Buffer+=format((b&255)+256,'x')[1:]
12
13 def m2(str):
14     messageDigest = hash.sha256()
15     bytes = str.encode("UTF-8")
16     messageDigest.update(bytes)
17     return messageDigest.digest()
18
19 m2131c = m2(str_Buffer)
20 iv=bytes([0]*16)
21 byte = str_Buffer.encode("UTF-8")
22 cipher = AES.new(m2131c, AES.MODE_CBC, iv)
23 encrypted_byte = cipher.encrypt(pad(byte, AES.block_size))
24 sql_key = base64.b64encode(encrypted_byte).decode("UTF-8")
25
26 print(sql_key)
```

```
-- 'C:\Users\Jin_Cheol\Documents\FaS\7발표\dec.py'
```

```
hyC+MnqlGLxSaSHyez77pJ9u+0jYS4kDvekYf9BCXMAxbP1ex2k90MnquurkIVRntNuCAzZYrBoOxToZWdEoXyGwX7Up6ae17h9M85PsFeQ=
```

Send a message



+ New chat



Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# DB 복호화 - 3. 키 획득 및 복호화



DB Browser for SQLite - C:\Users\Wjin\_Cheol\Documents\FaS\8발표\TeamUP\_v5.db

파일(F) 편집(E) 보기(V) 도구(T) 도움말(H)

새 데이터베이스(N)

데이터베이스 열기(O)

변경사항 저장하기(W)

변경사항 취소하기(R)

프로젝트 열기(P)

데이터베이스 연결(A)

데이터베이스 구조

데이터 보기

Pragma 수정

SQL 실행

테이블 생성하기(C)

인덱스 생성하기(I)

인쇄하기

이름	타입	스키마
테이블 (20)		
DepartmentInfo		CREATE TABLE DepartmentInfo (team_index INTEGER, idx INTEGER, name TEXT)
Feed		CREATE TABLE Feed (team INTEGER, feedgroup INTEGER, groupname TEXT, group_index INTEGER, feed_index INTEGER, feed_group_favorite INTEGER, feed_group_thumb INTEGER)
FeedGroup		CREATE TABLE FeedGroup (team INTEGER, feed_group INTEGER, group_name TEXT, feed_group_favorite INTEGER, feed_group_thumb INTEGER)
FeedGroupFavorite		CREATE TABLE FeedGroupFavorite (team_index INTEGER, feed_group_index INTEGER, feed_index INTEGER, feed_group_favorite INTEGER)
FeedGroupThumb		CREATE TABLE FeedGroupThumb (feed_group_id INTEGER, team_id INTEGER, feed_index INTEGER, feed_group_thumb INTEGER)
FileInfo		CREATE TABLE FileInfo (id TEXT, feed_index INTEGER, file_type_media TEXT, file_type_image TEXT, file_type_video TEXT, file_type_audio TEXT, file_type_text TEXT, file_type_other TEXT, file_type_unknown TEXT)
FileThumb		CREATE TABLE FileThumb (feed_file_id TEXT, child_path TEXT, host TEXT, UN
FixedFeedGroups		CREATE TABLE FixedFeedGroups (fixed_feed_group INTEGER, UNIQUE(fixed_
MessageInfo		CREATE TABLE MessageInfo (team INTEGER, room INTEGER, msg INTEGER, s
MyInfo		CREATE TABLE MyInfo (Lock char(1) not null DEFAULT 'X', idx INTEGER, nam
News		CREATE TABLE News (team_index INTEGER, feedgroup_index INTEGER, group
Notild		CREATE TABLE Notild (type INTEGER, feed INTEGER, noti_id INTEGER, room I
RoomInfo		CREATE TABLE RoomInfo (team INTEGER, roomtype INTEGER, room INTEGER
RoomReadCount		CREATE TABLE RoomReadCount (_id INTEGER PRIMARY KEY AUTOINCREMEN
RoomRemoveCount		CREATE TABLE RoomRemoveCount (room INTEGER, cnt INTEGER, UNIQUE(rc
TeamInfo		CREATE TABLE TeamInfo (idx INTEGER NOT NULL, name TEXT, status STATUS
TeamProfile		CREATE TABLE TeamProfile (idx INTEGER, name TEXT, status TEXT, roles TEX
Timestamp		CREATE TABLE Timestamp (idx INTEGER, type TEXT, last_update_time INTEGE
UserInfo		CREATE TABLE UserInfo (idx INTEGER, email TEXT, name TEXT, birthday TEX
sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)
인덱스 (11)		
DepartmentInfo_index1		CREATE INDEX DepartmentInfo_index1 ON DepartmentInfo(team_index,parent
MessageInfo_index1		CREATE INDEX MessageInfo_index1 ON MessageInfo(room,team,state,msg)
MessageInfo_index2		CREATE INDEX MessageInfo_index2 ON MessageInfo(room,team,state,filetype
Notild_index1		CREATE INDEX Notild_index1 ON Notild(type,feed)
RoomInfo_index1		CREATE INDEX RoomInfo_index1 ON RoomInfo(state,name)
RoomInfo_index2		CREATE INDEX RoomInfo_index2 ON RoomInfo(name)
RoomReadCount_index1		CREATE INDEX RoomReadCount_index1 ON RoomReadCount(team,room)

데이터베이스 셀 수정하기(C)

모드: 문자열

NULL

현재 데이터 타입: 널  
0 바이트

원격(R)

신원 연결할 ID를 선택하세요

DBHub.io

로컬

현재 데이터베이스

이름

마지막 수정

크기

&lt;

&gt;

SQL 로...

플...

DB 스카...

원...

암호화됨 UTF-8

2. TeamUP 복호화

× +

← → ↺

kookmin univ.

⋮

+ New chat

☐

Today

💬

폰 루팅

💬

팀업 복호화

💬

문제 초안

👤 FaS 세미나

20192233 박진철

데이터베이스 속 정보

🔍

MessageInfo 테이블에 보낸 채팅 내역 저장

데이터베이스 구조   데이터 보기   Pragma 수정   SQL 실행

테이블(T): MessageInfo

모든 열에서 필터링

	team	room	msg	state	user	type	len	content	tagfeeds	created	files	filetype	users
	필터	필터	필터	필터	필터	필터	...	필터	필터	필터	필터	필터	필터
1	23869	1540107	582386121	4	109000	7	6	ㅎㅎㅎㅎㅎ	[]	1685633047 {"chatcount":...		1	[]
2	23869	1540107	582386124	4	109000	7	5	hello	[]	1685633053 {"chatcount":...		1	[]
3	23869	1540107	582386158	4	109000	8	0		[]	1685633109 {"chatcount":...		1	[]
4	23869	1540107	582386159	4	109000	8	0		[]	1685633109 {"chatcount":...		1	[]
5	23869	1540107	582386161	4	109000	8	0		[]	1685633109 {"chatcount":...		1	[]
6	23869	1540107	582388498	4	108999	1	16	앗 이제 봤어 ㅋㅋㅋ 하이하이	[]	1685653941 {"chatcount":...		1	[]
7	23869	1540107	582386160	4	109000	8	0		[]	1685633109 {"chatcount":...		2	[]
8	23869	1546448	584868653	4	109269	1	14	진하~(진철 하이라는 뜻)	[]	1686656589 {"chatcount":...		1	[]
9	23869	1546448	584868699	4	109269	1	13	오리를 생으로 먹으면은?	[]	1686656633 {"chatcount":...		1	[]
10	23869	1546448	584868704	4	109269	1	3	회오리	[]	1686656636 {"chatcount":...		1	[]
11	23869	1546448	584868715	4	109269	1	5	꽤하하하하	[]	1686656645 {"chatcount":...		1	[]
12	23869	1546448	585864513	4	109000	7	3	ㅋㅋㅋㅋ	[]	1686909522 {"chatcount":...		1	[]
13	23869	1546448	585864531	4	109000	8	0		[]	1686909537 {"chatcount":...		1	[]

Send a message

2. TeamUP 복호화

kookmin univ.

+ New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

데이터 베이스 속 정보

MessageInfo

 테이블에 보낸 채팅 내역 저장

테이블(T): UserInfo

	idx	email	name	birthday	profile_image	message	status	mobile	mobile_numeric	phone	phone_num
	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	109000	ic1595@kookmi...	박진철	NULL			approval				
2	108999	wh ehdgn1001@...	조동후	NULL	https://...		approval				
3	109269	okstroy0522@g...	김강한	NULL			approval				
4	109274	wgx0805@naver...	정현태	NULL			approval				

UserInfo 테이블에서 User 정보 획득 가능

Send a message

2. TeamUP 복호화

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

데이터 베이스 속 정보

MessageInfo 테이블에 보낸 채팅 내역 저장

실행

모든 열에서 필터링

content

필터

ㅎㅇㅎㅇㅎㅇ

hello

앗 이제 봤어 ㅋㅋㅋ 하이하이

진하~(진철 하이라는 뜻)

오리를 생으로 먹으면은?

회오리

팩하하하하

꺄꺄꺄

Content 속성에서 메시지 내용 확인 가능

Send a message

2. TeamUP 복호화

kookmin univ.

+ New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

데이터 베이스 속 정보

MessageInfo 테이블에 보낸 채팅 내역 저장

	tagfeeds	created	files	filetype	users	extras	parent_message	vote
1	[필터]	1685633047	{"chatcount":...	1	[필터]			
2	[필터]	1685633053	{"chatcount":...	1	[필터]			
3	[필터]	1685633109	{"chatcount":...	1	[필터]			
4	[필터]	1685633109	{"chatcount":...	1	[필터]			
5	[필터]	1685633109	{"chatcount":...	1	[필터]			
6	[필터]	1685653941	{"chatcount":...	1	[필터]			
7	[필터]	1685633109	{"chatcount":...	2	[필터]			
8	[필터]	1686656589	{"chatcount":...	1	[필터]			
9	[필터]	1686656633	{"chatcount":...	1	[필터]			
10	[필터]	1686656636	{"chatcount":...	1	[필터]			
11	[필터]	1686656645	{"chatcount":...	1	[필터]			
12	[필터]	1686909522	{"chatcount":...	1	[필터]			
13	[필터]	1686909537	{"chatcount":...	1	[필터]			
14	[필터]	1687197232	{"chatcount":...	1	[필터]			
15	[필터]	1687197238	{"chatcount":...	1	[필터]			
16	[필터]	1687197244	{"chatcount":...	1	[필터]			

데이터베이스 구조

데이터 보기

Pragma 수정

SQL 실행

모든 열에서 필터링

데이터베이스 셀 수정하기(C)

모드: JSON

```
"newjeans-all-members-omg-album-shoot-wallpaper-3440x1440_15.jpg", "notecount": 0, "owner": 109000, "parent": 0, "reply": 0, "room": 1540107, "size": 557522, "thumbnail": {"host": "images.tmup.com", "path": "/KKg/AanI/NAI/XT0/EW8/8__Z5PtCLYYA8ZkRC6mQbQ.jpg",
```

현재 데이터 타입: 유효한 JSON

407 자

원격(R)

신원 연결할 ID를 선택하세요

DBHub.io 로컬 현재 데이터베이스

이름 마지막 수정 크기

files

필터

```
{"chatcount":...}
```

Files 속성에서 첨부파일의 썸네일 확인 가능

Send a message

+ New chat

Today

폰 루팅

팀업 복호화

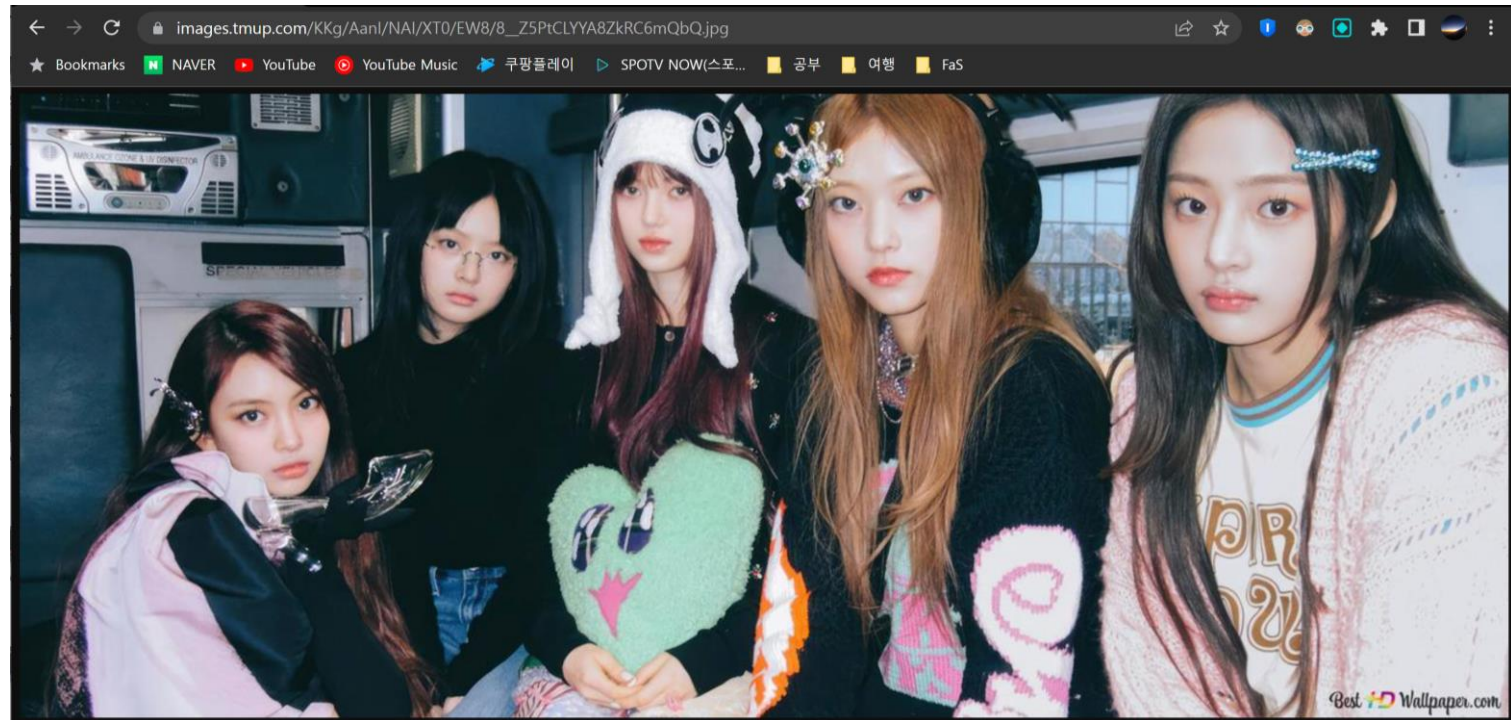
문제 초안

FaS 세미나

20192233 박진철

# 데이터 베이스 속 정보

MessageInfo 테이블에 보낸 채팅 내역 저장



Files 속성에서 첨부파일의 썸네일 확인 가능

Send a message



## 파일시스템 문제 - 삭제된 파일 복원

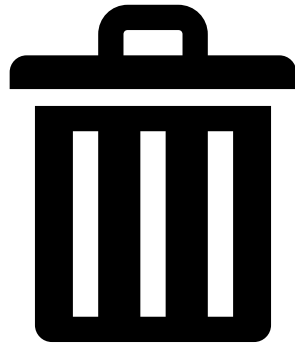


### 출제 의도

-이미지 파일을 주고 **삭제된 파일을 복원**하는 문제

-파일이 삭제될 경우

1. 파일의 디렉토리 엔트리의 **첫 바이트를 변경**
2. 새로운 파일이 저장되면 **디렉토리 엔트리에 새로운 파일의 정보가 쓰임**



-파일이 **데이터 영역에 남아있다면** 복원 가능  
→삭제된 파일의 **복원방법**을 알 수 있음

-난이도 **중~중상** 예상(데이터 카빙)

Send a message



+ New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# 파일시스템 문제 - 삭제된 파일 복원

## 문제 설계



-테러범의 계획을 찾는 문제

-제공되는 자료: 이미지 파일

1. 테러무기, 파일들에 대한 설명이 들어있는 텍스트 파일  
(삭제되지 않은 파일)

2. 테러범들의 인적사항이 기록된 텍스트 파일  
(삭제, 루트 디렉토리에는 정보 존재)

3. 테러를 하는 위치가 표시된 그림 파일  
(삭제, 루트 디렉토리에 정보 없음, 데이터 영역에는 존재)

-테러범의 인적사항과 테러 장소를 알아내면 성공

Send a message

3. 문제 초안

× +

← → ↺ kookmin univ.

+ New chat

☐

Today

💬 폰 루팅

💬 팀업 복호화

💬 문제 초안

👤 FaS 세미나

20192233 박진철

# 파일시스템 문제 - 삭제된 파일 복원

## 🔍 문제 초안

경찰이 테러 조사 중 테러범의 도피처에서 **테러범의 계획이 숨겨져 있는 USB를 발견**하였다. 그러나 USB의 **중요한 파일은 삭제된** 상태였다. 경찰은 USB 전체를 **덤프 뜯 이미지**를 정보보안암호수학과 포렌식 수사관에게 전달하였다.

전달 받은 이미지에서 **삭제된 파일들을 복구**하여 **단서를 획득**하십시오. (풀이과정 포함)(HxD를 이용해 이미지를 분석)

Send a message ▶

+ New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

## 파일시스템 문제 - 삭제된 파일 복원

### 문제 초안

1. 덤프 뜯 이미지에서 **모든 파일을 추출**하시오  
-삭제가 안된 1번 파일을 찾아냄
2. **루트 디렉토리에서 삭제된 파일**을 찾아 단서를 획득하시오.  
-디렉토리 엔트리에서 첫번째 바이트가 0xE5인 파일을 찾음  
-이를 통해 2번 파일을 획득해야함
3. **데이터 카빙**을 이용해 삭제된 파일을 찾아 단서를 획득하시오.  
-1번 파일을 통해 jpg파일이라는 것을 알 수 있음  
-시그니처 카빙을 이용해 그림파일 획득

Send a message

+ New chat

Today

폰 루팅

팀업 복호화

문제 초안

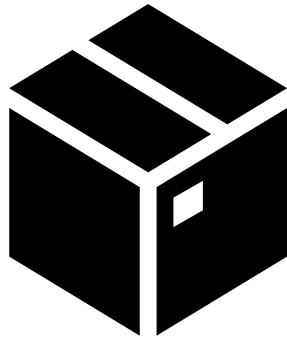
FaS 세미나

20192233 박진철

# 파일시스템 문제 - 은닉된 데이터 찾기



## 출제 의도



-이미지 파일을 주고 은닉된 정보를 찾는 문제

-파일시스템에는 낭비되는 영역이 존재

1. 슬랙
2. 배드 블록
3. 예약된 공간 등

-탐지가 어려운 영역에 파일을 은닉 가능  
→은닉 파일을 찾는 안티안티포렌식을 알 수 있음

-난이도 중 예상

Send a message

+ New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# 파일시스템 문제 - 삭제된 파일 복원



## 문제 설계

-은닉된 시험 정보를 찾는 문제



-제공되는 자료: 이미지 파일

1. 예약영역에 정보 은닉 (시험 날짜)
2. 램슬랙에 정보 은닉 (시험 장소)
3. 파일시스템슬랙에 정보 은닉 (시험 범위)
4. Bad Cluster에 데이터 은닉 (시험 기출문제)

-은닉된 데이터를 찾아내면 성공

Send a message

3. 문제 초안

× +

← → ↺ kookmin univ.

+ New chat

☐

Today

💬 폰 루팅

💬 팀업 복호화

💬 문제 초안

👤 FaS 세미나

20192233 박진철

# 파일시스템 문제 - 삭제된 파일 복원

## 🔍 문제 초안

정보보안암호수학과 학부생 앨리스는 A과목을 재수강하였다. 개강날 교수님께서서는 USB를 덤프 뜯 이미지를 수강생들에게 주면서 "해당 **이미지 속에 시험에 대한 정보가 은닉**되어 있습니다."라고 말씀하셨다. 앨리스는 빨리 이미지 속의 정보를 획득하여 시험을 잘 봐야겠다는 결심을 했다.

전달 받은 이미지에서 **은닉된 파일을 찾아 시험에 대한 정보를 획득**하시오 (풀이과정 포함)(HxD를 이용해 이미지를 분석)

Send a message

3. 문제 초안

kookmin univ.

New chat

Today

폰 루팅

팀업 복호화

문제 초안

FaS 세미나

20192233 박진철

# 파일시스템 문제 - 삭제된 파일 복원

## 문제 초안

- 예약영역에 은닉되어 있는 정보를 찾아내시오.  
-시험 날짜를 찾아야 함
- 램슬랙에 은닉되어 있는 정보를 찾아내시오.  
-시험 장소를 찾아야 함
- 파일시스템슬랙에 은닉되어 있는 정보를 찾아내시오.  
-시험 범위를 찾아야 함
- Bad Cluster에 은닉되어 있는 정보를 찾아내시오.  
-시험 기출문제를 찾아야함

Send a message

마무리

×

+



kookmin univ.



00007



# 발표를 마치겠습니다!

다음은 시도:

- Q&A
- 문제 만들기
- 9차 세미나 준비